UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,173	01/16/2001	Russell Dellmo	GCSD-1131 (51211)	4910

74701 7590 03/04/2008

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST
255 S ORANGE AVENUE
SUITE 1401
ORLANDO, FL 32801

EXAMINER	
TRAN, TONGOC	

ART UNIT	PAPER NUMBER
2134	

NOTIFICATION DATE	DELIVERY MODE
03/04/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RUSSELL DELLMO, JAMES BERGMAN, and
DAVID W. HALL

Appeal 2007-3601
Application 09/761,173
Technology Center 2100

Decided: February 29, 2008

Before JOSEPH L. DIXON, ALLEN R. MACDONALD, and
STEPHEN C. SIU, *Administrative Patent Judges*.

SIU, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1-51. We have jurisdiction under 35 U.S.C. § 6(b). We affirm-in-part.

A. Invention

1The invention at issue involves a secure wireless device (Spec. 3). In particular, a wireless device is rendered tamper-resistant such that stored cryptography information is rendered unuseable upon tampering of the device (*id.* 15).

B. Illustrative Claims

Claim 1, which further illustrates the invention, follows:

1. A secure wireless local area network (LAN) device comprising:

a housing;

a wireless transceiver carried by said housing;

a media access controller (MAC) carried by said housing; and

a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver, said cryptography circuit operating using cryptography information and rendering unuseable the cryptography information based upon tampering.

C. Rejection

Claims 1-6, 8, 10, 13-18, 21, 24-28, 30-34, 36-41, and 43-50 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,480,477 ("Treadaway"), U.S. Patent Publication No. 2001/0021926 ("Schneck"), and U.S. Patent No. 6,259,933 ("Bambridge").

Claims 7, 9, 19, 20, 29, 35, 42, and 51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Treadaway, Schneck, Bambridge, and U.S. Patent No. 6,560,448 ("Baldwin").

Claims 11 and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Treadaway, Schneck, Bambridge, and U.S. Patent Publication No. 2002/0114288 ("Soliman").

Claims 12 and 23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Treadaway, Schneck, Bambridge, and U.S. Patent No. 6,665,285 ("Treadaway '285").

PRINCIPLES OF LAW

Section 103 within Title 35 of the U.S. Code "forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1734 (2007); (quoting 35 U.S.C. § 103). "Determination of obviousness under 35 U.S.C. § 103 is a legal conclusion based on underlying facts." *In re Kumar*, 418 F.3d 1361, 1365 (Fed. Cir. 2005). This court reviews "the Board's ultimate determination of obviousness de novo." *In re Kotzab*, 217 F.3d 1365, 1369 (Fed. Cir. 2000). However, the Board's underlying findings of fact receive review for substantial evidence. *Id.* "If the evidence in [the] record will support

several reasonable but contradictory conclusions, we will not find the Board's decision unsupported by substantial evidence simply because the Board chose one conclusion over another plausible alternative." *In re Jolley*, 308 F.3d 1317, 1320 (Fed. Cir. 2002).

II. CLAIM GROUPING

1"When multiple claims subject to the same ground of rejection are argued as a group by Appellants, the Board may select a single claim from the group of claims that are argued together to decide the appeal with respect to the group of claims as to the ground of rejection on the basis of the selected claim alone. Notwithstanding any other provision of this paragraph, the failure of Appellants to separately argue claims which Appellants have grouped together shall constitute a waiver of any argument that the Board must consider the patentability of any grouped claim separately." 37 C.F.R. § 41.37(c)(1)(vii) (2005).[1]

Appellants argue claims 1-6, 8, 10, 36-41, 43-50 as a first group (App. Br. 6-14 and 19-22),[2] claims 13-18 and 21 as a second group (*id.* 14-16); claims 24-28 as a third group (*id.* 16-17); and claims 30-34 as a fourth group (*id.* 17-19). We select claim 1 as the sole claim on which to decide the

[1] We cite to the version of the Code of Federal Regulations in effect at the time of the Appeal Brief. The current version includes the same rules.

[2] Appellants place claims 36-41 and 43-50 in different headings in the Appeal Brief, but rely on the same arguments with respect to deficiencies in Treadaway and Schneck as applied against claim 1.

appeal of the first group and claim 13 as the sole claim on which to decide the appeal of the second group. Dependent claims 7, 9, 42, and 51 rejected over Treadaway, Schneck, Bambridge, and Baldwin; dependent claim 11 rejected over Treadaway, Schneck, Bambridge and Soliman; and dependent claim 12 rejected over Treadaway, Schneck, Bambridge, and Treadway '285 will stand or fall with base claim 1. Dependent claims 19 and 20 rejected over Treadaway, Schneck, Bambridge, and Baldwin; dependent claim 22 rejected over Treadaway, Schneck, Bambridge and Soliman; and dependent claim 23 rejected over Treadaway, Schneck, Bambridge, and Treadway '285 will stand or fall with base claim 13. We consider separately the appeal of claims 24-35.

III. CLAIMS 1-12 AND 36-51

As set forth above, we select claim 1 as the sole claim on which to decide the appeal of the first group. Rather than reiterate the positions of parties *in toto*, we focus on the issue therebetween.

Appellants argue that one of ordinary skill in the art "would have been taught away from making the suggested combination (of Treadaway and Schneck)" (App. Br. 10) because "the encryption/decryption block 612 of the [Treadaway] . . . patent teaches dual encryption and decryption" while Schneck discloses that "the access mechanism 114 decrypts pre-encrypted packaged data 108" (App. Br. 10). Based on this contention, Appellants

conclude that Schneck "teaches away from mutual encryption/decryption of data packets, as required by the [Treadaway] . . . patent" (App. Br. 10-11).

"A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994); *see KSR*, 127 S. Ct. at 1739–40 (explaining that when the prior art teaches away from a combination, that combination is more likely to be nonobvious). Treadaway discloses a method and apparatus for transmitting data securely using "an encryption/decryption block **612**" (col. 23, l. 48) such that "data security is enhanced" (col. 23, l. 67) as compared to a configuration without encryption (Fig. 4). Similarly, as Appellants indicate, Schneck discloses a method and apparatus for transmitting data securely using encryption and decryption of data. Although Treadaway discloses one example in which an "encryption/decryption block **612**" that both "encrypts the Ethernet data packets" and decrypts "Ethernet packets received from the link **102**" (col. 23, ll. 51-54), Treadaway does not preclude an embodiment in which separate components manage encryption and decryption. For example, Treadaway does not disclose that a decryption component separate from the encryption component would be detrimental or otherwise undesirable. Indeed, Treadaway discloses the need for an apparatus in which "data security is enhanced" (col. 23, l. 67) which

Appellants have not shown would be unachievable with the proposed modification.

Similarly, we do not find that Schneck discloses or suggests the undesirability of a combination component for encrypting and decrypting data. Rather, Schneck discloses one alternative in which encryption and decryption of data is performed in different components. As set forth above, Appellants have not provided a logical and convincing rationale as to how one of ordinary skill in the art would have been led in a direction divergent from using an alternative apparatus for encryption and decryption.

Thus, Appellants have failed to establish that modifying the Treadaway disclosure to incorporate an alternative in which encryption and decryption are accomplished using separate components (i.e., the Schneck disclosure) would defeat Treadaway's intent or purpose to enhance security. "The prior art's mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed . . ." *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004).

Appellants further argue that "[s]ince (Treadaway) . . . includes a continuous data flow system for signaling various components to ensure a continuous data flow rate across the wireless link **102**, one of ordinary skill in the art would be discouraged from combining the data packets or components within a closed, confined housing as suggested by . . . Schneck"

because "such teaching (of Schneck) is completely contrary to . . . (Treadaway)" (App. Br. 12).

As set forth above, Treadaway discloses a data transmission system in which data security is enhanced by encryption/decryption of the data. Schneck discloses data distribution and "controlling access to data by protecting portions of the data" (para. [0048]). Appellants have not established that whether the system is contained "within a closed, confined housing" or not would have any effect on encryption/decryption of data or data security. Nor have Appellants established a reason why one of ordinary skill in the art would have been led away from enclosing a data communication system within a housing. Therefore, based on the record before us, we cannot agree that one of ordinary skill in the art "would be discouraged from combining" Treadaway and Schneck as indicated by Appellants.

Appellants also argue that "there is no motivation or teaching to combine the references as suggested by the Examiner" (App. Br. 12) because Treadaway "includes no suggestion or motivation to combine with a tampering detection mechanism for packaged data sold to a user and secured within the physical bounds of an access laptop computer (*id*. 12-13). Based on this contention, Appellants assert that "the cited references do not disclose or fairly suggest the invention as set forth in independent claim 1 (*id*. 14).

We disagree. One of ordinary skill in the art, given the data transmission system with data encryption and decryption of Treadaway would have recognized the need for enhanced data security (*See* Treadaway, col. 23, l. 67). There is a finite number of ways in which one of ordinary skill in the art may provide security in a data transmission system. In one predictable scenario, security in a data transmission system may be breached upon tampering of any portion of the system. We identify one predictable solution to managing tampering of a data transmission system as including altering the system or the data based on detection of tampering in the system. Rendering data inaccessible upon detection of tampering would have been known to one of ordinary skill in the art, as demonstrated by Schneck, and would have produced expectedly predictable results – for example, maintaining data security in a data transmission system following tampering of a system component and a breach of security. Such anticipated success of using known methods to achieve expected results would have been obvious to one of ordinary skill in the art at the time of the invention. "When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense." *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1742 (2007). Moreover, we note that in *KSR*, the Supreme Court reaffirmed that "when a patent 'simply

arranges old elements with each performing the same function it had been known to perform' and yields no more than one would expect from such an arrangement, the combination is obvious." *KSR*, 127 S. Ct. at 1740 (quoting *Sakraida v. Ag Pro, Inc.*, 425 U.S. 273, 282 (1976)).

Thus, we agree with the Examiner that it would have been obvious to one of ordinary skill in the art, given the Schneck disclosure, to enhance security in the data transmission system of Treadaway using at least one of a finite number of methods including detecting tampering in the system and protecting data in response.

It follows that Appellants have failed to demonstrate that the Examiner erred in rejecting claim 1. Therefore, we affirm the rejection of claim 1 and of claims 2-6, 8, 10, 36-41, 43-50, which fall therewith. Claims 7, 9, 11, 12, 42, and 51, not separately argued by Appellants, also fall therewith.

IV. CLAIMS 13-23

As set forth above, we select claim 13 as the sole claim on which to decide the appeal of the second group.

Appellants argue Treadaway and Schneck fail to disclose "at least one connector 27 each carried by the housing for connecting to at least one of a LAN station 25 and a LAN access point 30" (App. Br. 15).

In response, the Examiner states that Treadaway teaches "the wireless link is coupled to the LAN (e.g., Fig. 3, item *108 (Connector)*, 106 (100

BASE-T, Ethernet standard and 212 (transceiver); Fig. 4, item 222 (MAC); and col. 7, lines 1-9)" (Ans. 12). The Examiner further states that "[s]ince it acts as an interface between the Logical Link and the network's *physical layer*, at least a connector connecting to a LAN station would have been obviously encompassed in the claimed device that comprise the MAC unit recited in claim 1 in order for the device to worked in the LAN environment as recited in the preamble" (Ans. 12).

Appellants do not refute the Examiner's findings. Therefore, Appellants have failed to demonstrate that the Examiner erred in rejecting claim 13.

Appellants also repeat arguments presented for independent claim 1. As set forth above, we find these arguments unpersuasive.

It follows that Appellants have failed to demonstrate that the Examiner erred in rejecting claim 13. Therefore, we affirm the rejection of claim 13 and of claims 14-18 and 21, which fall therewith. Claims 19, 20, 22, and 23, not separately argued by Appellants, also fall therewith.

V. CLAIMS 24-29 AND 30-35

Appellants argue that Treadaway and Schneck fail to disclose "at least one volatile memory **107** for storing the cryptography information and a battery **109** for maintaining the cryptography information in the at least one volatile memory" (App. Br. 16-19).

In response, the Examiner finds that Schneck discloses "the advantage of storing secure data in a volatile memory since data can not be retained once the power (or battery) is removed (Schneck, [0067], Office Action page 3)" (Ans. 11-12).

Although Schneck discloses a "[s]emiconductor memory" that "is volatile and does not retain data when power is removed" (para. [0067]), we do not find, and the Examiner fails to establish, that Schneck discloses a battery for maintaining cryptography information in the volatile memory as recited in claim 24 and claim 30. Schneck discloses a "long-life battery" that allows "rewriting (zeroizing) nonvolatile memory containing, for example, the private key" (*id.*). The system "must be returned to an authorized service facility for installation of a new private key" (*id.*). Because the private key must be re-installed at a service facility, we find that the battery of Schneck "zeroes" nonvolatile memory to eliminate the private key. This appears to be the opposite of using the battery for maintaining the private key in volatile memory as recited in claim 24 and claim 30.

Even assuming Schneck discloses advantages of storing data in volatile memory or that data is not retained if power is removed as the Examiner asserts, the Examiner has not demonstrated that Schneck discloses a "volatile memory for storing the cryptography information" and "a battery for maintaining the cryptography information in said . . . volatile memory" as recited in claim 24 and claim 30.

Therefore, we reverse the rejection of claims 24 and 30, and of claims 25-29 and 31-35, which depend therefrom.

VI. ORDER

In summary, the rejections of claims 1-23 and 36-51 under § 103(a) is affirmed. The rejection of claims 24-35 under § 103(a) is reversed.

No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

ce

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST, P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791